Threat Intelligence Research

SunCrypt Ransomware : Maze Re-incarnated

SunCrypt has made yet another iteration since its 2020 variant which was written in C post making first appearance in 2019. This time around they're catching up with other players by adopting novel methods. It claims to be a member of the Maze ransomware cartel and leverages several Maze methods, however the Maze ransomware gang has denied any affiliation. This ransomware group has impacted Corporates Educational Institute, University Hospital, Country School (US), Oklahoma City Indian Clinic (US), Mirgos (Switzerland) and healthcare systems mainly in USA and European countries.

Earlier this ransomware group adopted triple extortion technique; steal sensitive data, encrypt the servers, and threatens to launch distributed denial-of-service (DDoS) attack if the demands are not met. This group has come up with novel techniques such as process termination, stopping services, wiping the machine, and removing footprints by clearing the event logs through API Calls. It extracts fileless malware through an obfuscated PowerShell loader which is similar to "Netwalker PowerShell Loader scripts" and utilizes "ChaCha20" as a cryptographic method for encryption.

Once the script gets executed, it makes connection with the C2 server to communicate the victim's information prior to encryption. Once encrypted, all the files are appended with their hexadecimal hash as the extension and a ransom note is dropped in multiple languages like English, German, French, Spanish and Japanese, instructing the methods to pay ransom. SunCrypt hosts a leak site to extort the victims into paying the ransom. Given the group is progressively increasing the attack frequency with new variants and TTPs, regular security updates of systems is key to mitigate such threats.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

What is KPMG Cyber Threat Intelligence Platform (CTIP)?

The KPMG Threat Intelligence Platform (CTIP) is an industry defining, research-based capability for enhanced visibility into cyber threats. Our machine ingestible feeds are the result of automated, sensor-based intelligence metrics with dedicated, expert analysis of each threat to provide you the right context on a timely basis in industry standard formats such as STIX/ TAXII/ MISP. These feeds are additionally co-related with out industry partners and independent researchers to ensure you have the most accurate and contextual data. The intelligence is then curated from Strategic, Tactical and Operational perspective to give you 360 degree view of cyber threats.

We also assist you with our renowned **Cyber Incident Response** and **Threat Hunting services** in case you identify an active threat in your environment.

Range of services
Strategic Threat Intelligence Report
Machine Ingestible Threat Intelligence feeds
Threat Intelligence driven pre-emptive Threat Hunting Exercise
Cyber Incident Response Services

Contact us

KPMG Cyber Response Hotline : +91 9176 471 471

Atul Gupta
Partner, Head of Cyber Security, KPMG India
+91 98100 81050
atulgupta@kpmg.com

B V, Raghavendra
Partner, KPMG India
+91 98455 45202
raghavendrabv@kpmg.com

Sony Anthony
Partner, KPMG India
+91 98455 65222
santhony@kpmg.com

Chandra Prakash
Partner, KPMG India
+91 99000 20190
chandraprakash@kpmg.com

Manish Tembhurkar
Associate Partner, KPMG India
+91 98181 99432
mtembhurkar@kpmg.com

Rishabh Dangwal
Associate Director, Cyber Security
+91 78277 54752
rishabhd@kpmg.com

Threat Intelligence Research

SunCrypt Ransomware : Maze Re-incarnated

Indicators of Compromise

IP Addresses	
91.218.114[.]31	91.218.114[.]30

Domains	
onlygift[.]ga	ns1.showingemail[.]info
nesinoder[.]com	nbzzb6sa6xuura2z[.]onion
ns2.parens[.]ru	ebwexiymbsib4rmw[.]onion
ns1.parens[.]ru	2dehandsklant.onlygift[.]ga
2dehands.onlygift[.]ga	2dehandscontrole.onlygift[.]ga
ns2.showingemail[.]info	

Hashes
37e9bbf241ee93b3a32f8369b4c3d717
93e0b55df61b794d6e2e61a76376837e
93543af2c5f271d78492412a2ba99898
d87fcd8d2bf450b0056a151e9a116f72
3721354256c68818c9d0b5cb349a73d3
18923bfd1014231d456ce2d53c40c234
4aee8615dc8f4413f38adb2f17fd3fe9
c171bcd34151cbcd48edbce13796e0ed
479712042d7ad6600cbe2d1e5bc2fa88
0a0882b8da225406cc838991b5f67d11
3d756f9715a65def4a302f5008b03809
d87fcd8d2bf450b0056a151e9a116f72
264fa451fde41b44af005661e56c3a36758b9437
95c973dc078eac59198bb3047961a39cda278957
fbee2c987e310fc8be3d4efcf83cf5d4e76328e1
48cb6bdbe092e5a90c778114b2dda43ce3221c9f
88cce011722b593289826b1be01e6f47c4c15fb4
35e0f1c87b7823f8e8f465eeff0304724bdf0648
f1c7c1033e30527312a099ca3b7e6955fafd6c9e
48cb6bdbe092e5a90c778114b2dda43ce3221c9f
a9abb1e3d1060abac6830b591f2f4805b401fc4220b6f85f9ffdc7c26748e4bb
a52a8d8f92438bea70563f51da313f60aabd0fbbe8701a7ed4205f6f38acdf02

KPMG

Threat Intelligence Research

SunCrypt Ransomware : Maze Re-incarnated

Indicators of Compromise

Hashes
763b713938e62c036fa8f010cc3ac5f202be649e32a3ab5a2052da613e61643d
6d39b67805c6c17ab950679e752d9a947de4e911034a1c9c63473d40b5eee21c
6672c590317da13fa55f02b73ee737091922542ce29fd0514341c7d1f27b8d68
5bcef50ca8508939c361f0042e264f5e909ce2d8e949aa3db30fc81c1a8765b1
4b1f7e3323d797882d6082760592ea1984c29b975c1ae3c1daebf62dfb6a14e7
3090bff3d16b0b150444c3bfb196229ba0ab0b6b826fa306803de0192beddb80
0d7ed584dd1ae3cc071ad1b2400a5c534d19206be7a98a6046959a7267c063a1
de346f177e519b7d7942407ae5719b52ba446e46bf34bd7cf176889d4c3d6c57
c4329600329d3a3d75710f1d1006d45ca54fd362e86e26eba475724e113a1326
a5a0e5e73fc80dd5e70e1874a060b8a7c2c25b26aec5f54b123771a8535d1c56
996fec94a98ef61da2d8e8e7fb2ff5c7dd9f96b89f8cbf88baab6a45b7a5f013
81145757f3864fc085ee311c5237dc48216fa0a48b421329c8e75d94fe464e3f
7a84d10ac55622cdac25f52170459ae5b8181ee3fc345eb1b1dcbd958b344aa6
5f6cd6badb98e7fb6a9056b925e155b844073bbfbfe52e5576487440b1784b52
4acba1590552c9b2b82f5a786cedc8a12ca457e355c94f666efef99073827f89
45a74747c6728a9ee48b4550982ffcd19f257610bfcf73d26fb7781eac4a4365
24da3ccf131b8236d3c4a8cc29482709531232ef9c9cba38266b908439dea063
20ea5a9b5b2e47aa191132ac12c1d6dea6b58d7a0467ea53d48e96f8a79c6acd
18f03c65bf58549e8e230b8ef8595287fe51db0e5e411adfeaf261f87574543e
131341007b77fd077802a952889a75cbea81bf1f36afdc502388e9376f034ce4
11cbdb8216814198e99e251ecd8f4a1881900e345f75ef79731fd335e5099e05
03107d464f206320be5fa6ba9bcc304459fc86457681e9ad500c5c7875a9f304
f8441548dd050380d92790d05c9bcd853166fe30631ded525f77f7ddd00929da
e63c65e10f931a0fe4c6aeeb07e728fd7d6e1249d7cafdc6139faf0f7482e0b0
b72066c6ef651d5bebbb08bc51d3b6f73924e169ad93f7dd7530dbee3ff7e8a5
aa2316ff30647295efac2c884b30b6e83a8515c2d2ff1df3c5d6091b404c73a9
29b3f903c503c0a93e9f10524437ecb2f973a8e60879ca3cc974a6143a72cb9e
3090bff3d16b0b150444c3bfb196229ba0ab0b6b826fa306803de0192beddb80
63ba6db8c81c60dd9f1a0c7c4a4c51e2e56883f063509ed7b543ad7651fd8806
aa2316ff30647295efac2c884b30b6e83a8515c2d2ff1df3c5d6091b404c73a9
b4a13e327937fca9e23f8ed188259a24f84208782dde79ad0b3734cebe387c2b
ca5751036a12d0a9fba5f2c6cd2bde61b9c40e1607f751c39212b9c9a94c6b5a
e3dea10844aebc7d60ae330f2730b7ed9d18b5eec02ef9fd4a394660e82e2219
e63c65e10f931a0fe4c6aeeb07e728fd7d6e1249d7cafdc6139faf0f7482e0b0
E3DEA10844AEBC7D60AE330F2730B7ED9D18B5EEC02EF9FD4A394660E82E2219

Threat Intelligence Research

SunCrypt Ransomware : Maze Re-incarnated

Indicators of Compromise

Hashes
049af13ea1afabf23ee167d35411ebc5f019bac669242a4baed90643b999b31e
04bb145e3edea2cd19f3be102619c293c3ce685b03db53269668b568cff163e2
05d4a605de666f8c5ac8394e43cf18c8c6c53f926964e707301c7126a97c912e
0769845026e0e588d208aba408efbbdbf82a7309cbecf7ab4185472a32774d5b
08e9ca5519fc5bb14eaf6c1278fa62a9c653c075b6d9703ba10a4f4932e1a626
09710d371389a43eb242399fd5fc6ee042c1600ad3bbc1f65eba65a466f84d0d
0aca6ee0c21a890d3e9b1ef1289b5a0a83248a97a09d9e0b9f83e6a12d26d8a0
0b45d83f975e3589cf68db70282d4269dc0a4f8384e59f73242c9d614591ab47
0c0527adde005675cec50c743b55b1fb76ac8b09d33a37963bb35e2ed61f0430
0c6a102fdc91cc18528a12f26917bfc5ae49a72bc0f9dd02111a5036a8af92be
0d05cb821c142ac2cd3482a208ed0c31baa0aa07c5ff7879ed4c37ba164b7feb
0d7275152bc05939da8d2b66f1cf4755f48d11a505cdf9bebedbafa079fd9992
0de3273b0cbf615c2e69c2e6eff97572673fac47439345e9af04c01d3077c86e
10d41793b14bee85c06b4d68040e493a7cd018126e39f172efef10e79e835838
1124ba4b80ff399124920e0ec0c6c518af5b8e47a65afa4d1e6ace9c807240f7
1127a9d2ddcb9ee2837c6f823de42db69a0eadc2fd715d124fbdf68f25487242
116f867eb2c5a9915a28bcf033c8392d96ad7dcc95e207c877ad1eca72bf0833
130ca07368c1df3ecc1dd8d7f01764c227984a6ffac7b856e5659b6c19f49f4e
13386e03234bdd9f7958ecf55c37d5b92f2d867a2234025903b53d9e5c852ba7
E3DEA10844AEBC7D60AE330F2730B7ED9D18B5EEC02EF9FD4A394660E82E2219
0034ce69612de317c416788a11efd9427f62bed2d54ec5d59b2f02a12c7987d0